DAC

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
Washington, D.C. 20231
www.uspto.gov

SEP 30 2002
PATENT & TRADEMARK OFFICE

Dilip Gunawardena
827 Newport Circle
Redwood Shores, CA 94065

RECEIVED
OCT 0 8 2002
GROUP 3600

COPY MAILED
AUG 0 8 2002
OFFICE OF PETITIONS

In re Application of
James Kleinsteiber,
Richard L. Hammons,
Dilip Gunawardena, Hung Nguyen,
Shankar Balasubramanian, and
Vidya Renganararayanan
Application No. 10/062,125
Filed: January 31, 2002
Attorney Docket No. 112-0039US
Title: Network Security and
Applications to the Fabric

LETTER

Dear Dr. Gunawardena:

You are named as a joint inventor in the above-identified United States patent application filed under the provisions of 35 U.S.C. 116 (United States Code) and 37 CFR 1.47(a), Rules of Practice in Patent Cases. Should a patent be granted on the application you will be designated therein as a joint inventor.

As a named inventor you are entitled to inspect any paper in the file wrapper of the application, order copies of all or any part thereof (at a prepaid cost per 37 CFR 1.19) or make your position of record in the application. Alternatively, you may arrange to do any of the preceding through a registered patent attorney or agent presenting written authorization from you. If you care to join the application, counsel of record (see below) would presumably assist you. Joining in the application would entail the filing of an appropriate oath or declaration by you pursuant to 37 CFR 1.63.

Telephone inquiries regarding this communication should be directed to Petitions Attorney Nancy Johnson at (703) 305-0309. Requests for information regarding your application should be directed to the File Information Unit at (703) 308-2733. Information regarding how to pay for and order a copy of the application, or a specific paper in the application, should be directed to the Certification Division at (703) 308-9726 or 1-800-972-6382 (outside the Washington D.C. area).

Nancy Johnson
Petitions Attorney
Office of Petitions
Office of the Deputy Commissioner
for Patent Examination Policy

WONG, CABELLO, LUTSCH,
RUTHERFORD & BRUCCULERI, P.C.
20333 SH 249
SUITE 600
HOUSTON, TX 77070

RECEIVED
OCT 0 3 2002
OFFICE OF PETITIONS

Dilip Gunawardena
872 Newport Circle, Redwood Shores, CA 94065-1915
Email: dilip_gunawardena@yahoo.com
Telephone: 650-594-1360

September 5, 2002

Claims regarding patent application # 10/062,125 , Network Security and Applications to the Fabric Environment

Claim #1:
This claim is false.
"Operating a secure network" by "locating one or more nodes in a secure location", "locating one or more nodes in a less secure location", and "communicating selected management information from a primary configuration node to all other nodes in the secure network", is not an invention but mere common sense, doubtless practiced by millions of businesses on any given day.

Furthermore, the "communicating selected management information" sub-step #1 of "a first port on a first node sending said management information to a second port on a second node via a communication media exclusively shared by said first port and said second port" is not an invention but mere common sense, and consequently a widely-used business practice.

Furthermore, the "communicating selected management information" sub-step #2 of "allowing no management access to said secure network from nodes located in less secure locations" is not an invention but mere common sense, and consequently a widely-used business practice.

Furthermore, the "communicating selected management information" sub-step #3 of "determining a first list of nodes that may send or receive substantive communication in the secure network" is not a new invention. On the contrary, it is an Access Control List, which is fully defined in the following Internet Engineering Task Force (IETF) Request For Comments (RFC) specifications, all of which pre-date this patent application by several years:

- RFC 1157. Case, J., M. Fedor, M. Schoffstall, and J. Davin.
  A Simple Network Management Protocol.
  May 1990.

- RFC 1445. Glavin, J., and K. McCloghrie.
  Administrative Model for Version 2 of the Simple Network Management Protocol (SNMPv2).
  April 1993.

- RFC 2275. Wijnen, B., R. Presuhn, and K. McCloghrie. View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP). January 1998.

The aforementioned sub-step #3 of "determining a first list of nodes that may send or receive substantive communication in the secure network" has moreover been implemented, over the past several years, by every major Fibre Channel network switch manufacturer.

Furthermore, the "communicating selected management information" final sub-step #4 of "prior to substantive communication between any two directly-connected ports, authenticating a link between said directly connected ports" is not a new invention. On the contrary, it is a requirement whose necessity has been recognized for decades. In fact, one of many processes for fulfilling the above requirement is fully defined in "Entity Authentication Using Public Key Cryptography", FIPS PUB 196, 1997 February 18, US Department of Commerce / National Institute of Standards and Technology, which obviously pre-dates this patent application by several years.

Claims #2 to #21 inclusive:
Given the falsity of Claim #1, and given the dependency of Claims #2 to #21 inclusive upon Claim #1, Claims #2 to #21 inclusive are also false.

Claim #22:
This claim is false.
This process is fully defined in "Entity Authentication Using Public Key Cryptography", FIPS PUB 196, 1997 February 18, US Department of Commerce / National Institute of Standards and Technology, which obviously pre-dates this patent application by several years.

The aforementioned publication is derived from Section 5.2.2, "Three pass authentication", of ISO/IEC 9798-3, "Information technology – Security techniques – Entity Authentication – Part 3: Mechanisms using digital signature techniques", 1993 and 1998, which obviously pre-date this patent application by several years.

Claims #23 to #34 inclusive:
Given the falsity of Claim #22, and given the dependency of Claims #23 to #34 inclusive upon Claim #22, Claims #23 to #34 inclusive are also false.

Claim #35:
This claim is false.

Any network node in general will invariably contain "a first port", "a second port", "a memory" and "a processor".

Furthermore, "authentication of the link between said first port and said second port prior to substantive communication between said first and second ports" is not a new invention. On the contrary, it is a requirement whose necessity has been recognized for decades. In fact, one of many processes for fulfilling the above requirement is fully defined in "Entity Authentication Using Public Key Cryptography", FIPS PUB 196, 1997 February 18, US Department of Commerce / National Institute of Standards and Technology, which obviously pre-dates this patent application by several years.

Claims #36 to #55 inclusive:
Given the falsity of Claim #35, and given the dependency of Claims #36 to #55 inclusive upon Claim #35, Claims #36 to #55 inclusive are also false.

Claim #56:
Given the falsity of Claim #35, and given the dependency of Claim #56 upon Claim #35, Claim #56 is also false.

Furthermore, this process is fully defined in "Entity Authentication Using Public Key Cryptography", FIPS PUB 196, 1997 February 18, US Department of Commerce / National Institute of Standards and Technology, which obviously pre-dates this patent application by several years.

The aforementioned publication is derived from Section 5.2.2, "Three pass authentication", of ISO/IEC 9798-3, "Information technology – Security techniques – Entity Authentication – Part 3: Mechanisms using digital signature techniques", 1993 and 1998, which obviously pre-date this patent application by several years.

Claims #57 to #61 inclusive:
Given the falsity of Claim #56, and given the dependency of Claims #57 to #61 inclusive upon Claim #56, Claims #57 to #61 inclusive are also false.

Claim #62:
This claim is false.
The "method of securing said network", step #1 of "mutually authenticating all links in the network" is not an invention but mere common sense, because all links in the network must be securely authenticated before the network can be said to be secure.

Furthermore, mutual authentication of two nodes on a link is not a new invention. On the contrary, it is a requirement whose necessity has been recognized for decades. In fact, one of many processes for fulfilling the above requirement is fully defined in "Entity

Authentication Using Public Key Cryptography", FIPS PUB 196, 1997 February 18, US Department of Commerce / National Institute of Standards and Technology, which obviously pre-dates this patent application by several years.

The "method of securing said network", step #2 of "limiting access to a first set of one or more management functions by allowing control of said first set of management functions only through one or more pre-selected devices", and step #3 of "limiting access to a second set of management functions to access only through one or more pre-determined logical channels of said devices as specified by a network operator", are not new inventions. On the contrary, they constitute an Access Control List, which is fully defined in the following Internet Engineering Task Force (IETF) Request For Comments (RFC) specifications, all of which pre-date this patent application by several years:

- RFC 1157. Case, J., M. Fedor, M. Schoffstall, and J. Davin.
  A Simple Network Management Protocol.
  May 1990.

- RFC 1445. Glavin, J., and K. McCloghrie.
  Administrative Model for Version 2 of the Simple Network Management Protocol (SNMPv2).
  April 1993.

- RFC 2275. Wijnen, B., R. Presuhn, and K. McCloghrie.
  View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP).
  January 1998.

Furthermore, the aforementioned steps #2 and #3 have moreover been implemented, over the past several years, by every major Internet Protocol network router manufacturer and every major Fibre Channel switch manufacturer.

Claims #63 to #68 inclusive:
Given the falsity of Claim #62, and given the dependency of Claims #63 to #68 inclusive upon Claim #62, Claims #63 to #68 inclusive are also false.

Claim #69:
This claim is false.
The "method of Claim #62 further comprising the step of providing a distributed time service" is not a new invention.
This process is fully defined in "Entity Authentication Using Public Key Cryptography", FIPS PUB 196, 1997 February 18, US Department of Commerce / National Institute of Standards and Technology, which obviously pre-dates this patent application by several years.

The aforementioned publication is derived from Section 5.2.2, "Three pass authentication", of ISO/IEC 9798-3, "Information technology – Security techniques – Entity Authentication – Part 3: Mechanisms using digital signature techniques", 1993 and 1998, which obviously pre-date this patent application by several years.

Claim #70:

This claim is false.

The said distributed time service is not a new invention. On the contrary, it is fully defined, as part of the Network Time Protocol (NTP), in the following Internet Engineering Task Force (IETF) Request For Comments (RFC) specifications, all of which pre-date this patent application by several years:

- RFC 2030: Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI.
  D. Mills.
  October 1996.

- RFC 1708: NTP PICS PROFORMA - For the Network Time Protocol Version 3.
  D. Gowin.
  October 1994.

- RFC 1305: Network Time Protocol (Version 3) Specification, Implementation.
  D. Mills.
  March 1992.

- RFC 1129 Internet Time Synchronization: The Network Time Protocol.
  D. L. Mills.
  Oct-01-1989.

- RFC 1165 Network Time Protocol (NTP) over the OSI Remote Operations Service.
  J. Crowcroft, J.P. Onions.
  Jun-01-1990.

Claim #71:

This claim is false.

The "method of Claim #62 wherein the network comprises a Fibre Channel fabric" is not a new invention. On the contrary, it constitutes an Access Control List, which is fully defined in the following Internet Engineering Task Force (IETF) Request For Comments (RFC) specifications, all of which pre-date this patent application by several years:

- RFC 1157. Case, J., M. Fedor, M. Schoffstall, and J. Davin.
  A Simple Network Management Protocol.

May 1990.

- RFC 1445. Glavin, J., and K. McCloghrie.
  Administrative Model for Version 2 of the Simple Network Management Protocol (SNMPv2).
  April 1993.

- RFC 2275. Wijnen, B., R. Presuhn, and K. McCloghrie.
  View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP).
  January 1998.

Furthermore, the aforementioned "method of Claim #62 wherein the network comprises a Fibre Channel fabric" has moreover been implemented over the past several years by every major Fibre Channel switch manufacturer.

Claim #72:

This claim is false.

The said "method of securing a fabric, said fabric having a plurality of switches all communicatively coupled together", step #1 of "only allowing communication between pre-defined pairs of said devices as specified by a network operator", and step #2 of "only allowing substantive communication between devices that are on a pre-defined list of allowed devices, said pre-defined list stored on a memory in each of said plurality of devices", are not new inventions. On the contrary, they constitute an Access Control List, which is fully defined in the following Internet Engineering Task Force (IETF) Request For Comments (RFC) specifications, all of which pre-date this patent application by several years:

- RFC 1157. Case, J., M. Fedor, M. Schoffstall, and J. Davin.
  A Simple Network Management Protocol.
  May 1990.

- RFC 1445. Glavin, J., and K. McCloghrie.
  Administrative Model for Version 2 of the Simple Network Management Protocol (SNMPv2).
  April 1993.

- RFC 2275. Wijnen, B., R. Presuhn, and K. McCloghrie.
  View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP).
  January 1998.

Furthermore, the aforementioned steps #1 and #2 have moreover been implemented over the past several years by every major Fibre Channel switch manufacturer.

The said "method of securing a fabric, said fabric having a plurality of switches all communicatively coupled together", step #3 of "only allowing substantive communication between directly connected ports that have been mutually authenticated" is not an invention but mere common sense, because all directly-connected ports must be mutually authenticated over their common direct connection before the fabric can be said to be secure. Furthermore, mutual authentication over their common direct connection of directly-connected ports is not a new invention. On the contrary, it is a requirement whose necessity has been recognized for decades. In fact, one of many processes for fulfilling the above requirement is fully defined in "Entity Authentication Using Public Key Cryptography", FIPS PUB 196, 1997 February 18, US Department of Commerce / National Institute of Standards and Technology, which obviously pre-dates this patent application by several years.

Claim #73:

This claim is false.

The said network further comprising "one or more pre-designated devices for facilitating management-level control of the network", and in addition further comprising "all of said devices carrying a list of all devices allowed on the network", is not a new invention. On the contrary, it constitutes an Access Control List, which is fully defined in the following Internet Engineering Task Force (IETF) Request For Comments (RFC) specifications, all of which pre-date this patent application by several years:

- RFC 1157. Case, J., M. Fedor, M. Schoffstall, and J. Davin.
  A Simple Network Management Protocol.
  May 1990.

- RFC 1445. Glavin, J., and K. McCloghrie.
  Administrative Model for Version 2 of the Simple Network Management Protocol (SNMPv2).
  April 1993.

- RFC 2275. Wijnen, B., R. Presuhn, and K. McCloghrie.
  View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP).
  January 1998.

Claims #74 to #75 inclusive:

Given the falsity of Claim #73, and given the dependency of Claims #74 to #75 inclusive upon Claim #73, Claims #74 to #75 inclusive are also false.

Claim #76:

This claim is false.

Every Public Key Infrastructure (PKI)-enabled "routing device", from any manufacturer, invariably contains "a public and private key pair" as well as "one or more ports for coupling to other routing devices and for authenticating said other routing devices and for communicating using said public and private key pair". PKI-enabled routing devices have been manufactured by many companies over many years.

As for "authenticating said other routing devices", this is not a new invention. On the contrary, it is a requirement whose necessity has been recognized for decades. In fact, one of many processes for fulfilling the above requirement is fully defined in "Entity Authentication Using Public Key Cryptography", FIPS PUB 196, 1997 February 18, US Department of Commerce / National Institute of Standards and Technology, which obviously pre-dates this patent application by several years.

Furthermore, all routing devices require a "memory".

In the case of many routing devices, from many manufacturers, part of the aforementioned memory is used for "storing a list of all said other routing devices that are allowed to substantively communicate on the network". Many routing devices, from many manufacturers, also contain "at least one logical management access channel that may be disabled through network management control". Far from constituting new inventions, they constitute an Access Control List, which is fully defined in the following Internet Engineering Task Force (IETF) Request For Comments (RFC) specifications, all of which pre-date this patent application by several years:

- RFC 1157. Case, J., M. Fedor, M. Schoffstall, and J. Davin.
  A Simple Network Management Protocol.
  May 1990.

- RFC 1445. Glavin, J., and K. McCloghrie.
  Administrative Model for Version 2 of the Simple Network Management Protocol (SNMPv2).
  April 1993.

- RFC 2275. Wijnen, B., R. Presuhn, and K. McCloghrie.
  View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP).
  January 1998.

Claims #77 to #78 inclusive:
Given the falsity of Claim #76, and given the dependency of Claims #77 to #78 inclusive upon Claim #76, Claims #77 to #78 inclusive are also false.

Claim #79:
This claim is false.

Any "network configuration entity", from any manufacturer, invariably contains "a memory", "a processor", "a first port" and a second port". For many manufacturers' network configuration entities controlling management functions throughout a secure network, such management functions would include "the recognition, operation and succession of the network configuration entity" as well as facilities "for designating devices to participate in the secure network". They would also contain a list of all devices that might operate as a said network configuration entity, and a list of all devices allowed to participate in the said secure network.

The fact that network configuration entities can be used to store, send or receive a secret fact, derive a second-type and third-type derivative of that secret fact, and compare those facts, second-type derivatives, and third-type derivatives, is completely irrelevant. In fact for any Public Key Infrastructure (PKI) –enabled network switch attempting to mutually authenticate each of its ports with its neighbor on the other end of that link, this is a well-defined and commonly-used procedure. This procedure is fully defined in "Entity Authentication Using Public Key Cryptography", FIPS PUB 196, 1997 February 18, US Department of Commerce / National Institute of Standards and Technology, which obviously pre-dates this patent application by several years.

The aforementioned publication is derived from Section 5.2.2, "Three pass authentication", of ISO/IEC 9798-3, "Information technology – Security techniques – Entity Authentication – Part 3: Mechanisms using digital signature techniques", 1993 and 1998, which obviously pre-date this patent application by several years.

Claim #86:

Given the existence of Claim #87, Claim #86 is superfluous. That is because a nonce is a random number, to be used only once.

Claims #80 to #87 inclusive:

Given the falsity of Claim #79, and given the dependency of Claims #80 to #87 inclusive upon Claim #79, Claims #80 to #87 inclusive are also false.

Claim #88:

This claim is false.
The said "method of maintaining distributed time" is not a new invention. On the contrary, it is fully defined, as part of the Network Time Protocol (NTP), in the following Internet Engineering Task Force (IETF) Request For Comments (RFC) specifications, all of which pre-date this patent application by several years:

- RFC 2030: Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI.
  D. Mills.
  October 1996.

- RFC 1708: NTP PICS PROFORMA - For the Network Time Protocol Version 3.
  D. Gowin.
  October 1994.

- RFC 1305: Network Time Protocol (Version 3) Specification, Implementation.
  D. Mills.
  March 1992.

- RFC 1129 Internet Time Synchronization: The Network Time Protocol.
  D. L. Mills.
  Oct-01-1989.

- RFC 1165 Network Time Protocol (NTP) over the OSI Remote Operations Service.
  J. Crowcroft, J.P. Onions.
  Jun-01-1990.

Claim #89:

This claim is false.

The said "method of maintaining distributed time" is not a new invention. On the contrary, it is fully defined, as part of the Network Time Protocol (NTP) with digitally-signed time-stamps incorporated, in the following Internet Engineering Task Force (IETF) Request For Comments (RFC) specifications, all of which pre-date this patent application by several years:

- RFC 2030: Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI.
  D. Mills.
  October 1996.

- RFC 1708: NTP PICS PROFORMA - For the Network Time Protocol Version 3.
  D. Gowin.
  October 1994.

- RFC 1305: Network Time Protocol (Version 3) Specification, Implementation.
  D. Mills.
  March 1992.

- RFC 1129 Internet Time Synchronization: The Network Time Protocol.
  D. L. Mills.
  Oct-01-1989.

- RFC 1165 Network Time Protocol (NTP) over the OSI Remote Operations Service.
  J. Crowcroft, J.P. Onions.
  Jun-01-1990.

PEER REVIEW:

The falsity of the above claims will in all probability be corroborated and attested to by the following additional experts from the Fibre Channel industry:

(1)
Michael O'Donnell
McData Corporation
Email: modonnell@mcdata.com
Work address: Michael O'Donnell, McData Corporation, 310 Interlocken Parkway, Broomfield, CO 80021.

(2)
James Hughes
Chairperson, Storage Networking Industry Association (SNIA) Security Work Group
Email: hughes@network.com
Work address: James Hughes, Chairperson, SNIA Security Work Group, 2570 West El Camino Real, #304, Mountain View, CA 94040-1313.

(3)
Steven Dalton
CEO, Gadzoox Networks
Email: sdalton@gadzoox.com
Work address: Steven Dalton, Gadzoox Networks, 5850 Hellyer Avenue, San Jose, CA 95138.

(4)
Claudio DeSanti
Cisco Systems / Andiamo
Email: cds@andiamo.com
Work address: Claudio DeSanti, Cisco Systems / Andiamo, 375 East Tasman Drive, Building 6, Floor 3, San Jose, CA 95134.

(5)
Roger Cummings
Co-chairperson, Storage Industry Network Association (SNIA) Security Work Group
Veritas Corporation
Email: roger.cummings@veritas.com
Work address: Roger Cummings, Veritas Corporation, 350 Ellis Street, Mountain View, CA 94043.

(6)
Craig Carlson
Chairperson, InterNational Committee for Information Technology Standardization (INCITS) T11.3 Technology Group
QLogic Corporation
Email: craig.carlson@qlogic.com
Work address: Craig Carlson, QLogic Corporation, 26600 Laguna Hills Drive, Aliso Viejo, CA 92656.

Dilup Gunawardena